


UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	
v.	:	Hon. William J. Martini
	:	
KARLIS KARKLINS,	:	Criminal No. 11-299
a/k/a "Susanne O'Neill,"	:	
a/k/a "Kris,"	:	
a/k/a "Steven Bing,"	:	
CHARLES UMEH CHIDI,	:	
a/k/a "Charlie,"	:	<u>SEALING ORDER</u>
WAYA NWAKI,	:	
a/k/a "Jonh Done,"	:	
a/k/a "Prince Abuja,"	:	
a/k/a "Shawn Conley,"	:	
a/k/a "USAPrince12k,"	:	
OSARHIEME UYI OBAYGBONA,	:	
a/k/a "Uyi Obaygbona,"	:	
a/k/a "bside bside,"	:	
MARVIN DION HILL,	:	
a/k/a "Da Boss,"	:	
a/k/a "Nyhiar Da Boss,"	:	
a/k/a "Nihiar Springs,"	:	
ALPHONSUS OSUALA,	:	
a/k/a "Andrew Johnson,"	:	
a/k/a "jamal j," and	:	
OLANIYI JONES,	:	
a/k/a "Brenda Stuart,"	:	
a/k/a "Olaniyi Victor Makinde,"	:	
a/k/a "Makinde Olaniyi Victor"	:	

This matter having come before the Court upon the submission of an affidavit in support of extradition from the Republic of Nigeria of defendant Olaniyi Jones (Seth B. Kosto, Assistant U.S. Attorney, appearing) and its concurrent application that the affidavit and its attachments be filed under seal, and good cause having been shown,

IT IS, on this 11 day of August 2011,

ORDERED that, except for such copies of the affidavit as are necessary to accomplish their purpose, the affidavit is hereby SEALED until further order of the Court.



WILLIAM J. MARTINI
United States District Judge

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. William J. Martini
	:	
v.	:	Criminal No. 11-299 - 7
	:	
OLANIYI JONES,	:	AFFIDAVIT OF SETH B. KOSTO
a/k/a "Brenda Stuart,"	:	IN SUPPORT OF APPLICATION FOR
a/k/a "Olaniyi Victor Makinde,"	:	EXTRADITION OF OLANIYI JONES
a/k/a "Makinde Olaniyi Victor"	:	

et al.

I, Seth B. Kosto, being duly sworn, depose and state:

A. Basis for this Affidavit

1. I am a citizen of the United States and a resident of the State of New York.
2. I graduated from Boston College Law School in May 1998. Between August 1998 and September 1999, I was employed as a law clerk for the Honorable Zachary R. Karol, a United States Magistrate Judge of the United States District Court for the District of Massachusetts in Boston, Massachusetts. From October 1999 through February 2003, I was employed as an associate by Hill & Barlow in Boston, Massachusetts. From March 2003 through October 2005, I was employed as an associate by Holland & Knight LLP. Since then, I have been employed by the United States Department of Justice as an Assistant United States Attorney ("AUSA") for the District of New Jersey.
3. My duties as an AUSA include supervising the investigation and prosecution of persons charged with criminal violations of the laws of the United States. During my practice as an Assistant United States Attorney, I have become knowledgeable about the criminal laws and

procedures of the United States. Based upon my training and experience, I am an expert in the criminal laws and procedures of the United States.

4. In the course of my duties I have become familiar with the charges and the evidence in the case of *United States v. Karlis Karklins, Charles Chidi, Waya Nwaki, Osarhieme Obaygbona, Marvin Dion Hill, Alphonsus Osuala, and Olaniyi Jones*, filed in the United States District Court for the District of New Jersey in criminal case number 11-299. Olaniyi Jones is also charged with using the names “Brenda Stuart,” “Olaniyi Victor Makinde,” and “Makinde Olaniyi Victor” (hereafter “Jones”).

5. I have prepared this Affidavit in support of the United States’ request for the extradition of Jones based on the investigation conducted by the Department of Justice and the Federal Bureau of Investigation (“FBI”). This Affidavit does not identify all of the facts learned during the investigation. Rather, it includes specific information to summarize the case and to demonstrate probable cause to believe that Jones committed the offenses charged in the case above and described in this Affidavit. This information is derived from interviews of witnesses and documentary and electronic evidence, among other types of evidence developed during the FBI’s investigation.

B. The Charging Process

6. Under United States law, a criminal prosecution may be commenced by the filing of a criminal complaint as was initially done in this case. A criminal complaint is a written statement of the essential facts constituting the offense or offenses charged. The complaint also sets forth the charge or charges and the statutory citation for each offense alleged in the complaint. The complaint is presented to a judicial officer who must make a determination

whether the written statement of facts constitutes probable cause to believe that an offense has been committed and the person named as the defendant in the complaint committed the offense or offenses. If the judicial officer is satisfied that the complaint establishes probable cause to believe that an offense has been committed and the defendant committed it, the judge permits the complaint to be filed and, if appropriate, issues an arrest warrant for the defendant.

7. On December 14, 2010, a criminal complaint was filed in the United States District Court for the District of New Jersey charging Jones with conspiracy to commit wire fraud. The judicial officer also issued an arrest warrant on December 14, 2010 for Jones based upon the charges in the complaint.

8. Under United States law, a criminal prosecution may also be commenced by a grand jury when it votes to return and file an indictment with the Clerk of the United States District Court. If a case is initially charged by criminal complaint, the defendant must be ultimately charged by a grand jury for the case to proceed to trial. An indictment is a formal accusation or charging document issued by a grand jury. A grand jury consists of 16 to 23 citizens empaneled by the United States District Court to review evidence of crimes presented to it by U.S. law enforcement authorities. Each member of the grand jury must review the evidence presented and determine whether there is probable cause to believe that a crime has been committed and that it is likely that the accused person committed the crime. The grand jury may return an indictment charging the accused person with a crime when at least 12 grand jurors determine that it is more likely than not that the accused person committed the crime. Once the grand jury returns an indictment, it is filed with the Clerk of the United States District Court. In

addition, the grand jury can bring additional charges against the accused person (or add additional accused persons) using the same procedures to return a superseding indictment.

9. Here, Jones was named as one of seven defendants in a 27-count indictment, which was returned by the grand jury on April 28, 2011. It is the practice in the United States District Court for the District of New Jersey for the Clerk of Court to retain the originals of all complaints, indictments and warrants of arrest. Therefore, I have obtained a certified true and accurate copy of the indictment from the Deputy Clerk of Court, and have attached it to this affidavit as **Exhibit A**. In **Exhibit A**, the name of the foreperson of the grand jury has been redacted. The redaction of the name of the foreperson of the grand jury is pursuant to a general order from the United States District Court for the District of New Jersey. This order requires that any identifying information about jurors and grand jurors be redacted in the public case file to protect the privacy of those persons.

C. The Charges Against Jones and the Arrest Warrant

10. As seen in **Exhibit A**, the indictment, which contains 27 counts against all defendants, charges Jones with six separate offenses:

- a. conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349 (Count 1), which carries a maximum penalty of 20 years' imprisonment;
- b. wire fraud, in violation of 18 U.S.C. § 1343 (Counts 2 through 5), each count of which carries a maximum penalty of 20 years' imprisonment; and
- c. conspiracy to commit identity theft, namely to traffic in personal identifiers and log-in credentials, contrary to 18 U.S.C. § 1028(a)(7) and in violation of

18 U.S.C. § 1028(f) (Count 10), which carries a maximum penalty of 5 years' imprisonment.

11. After an indictment or superseding indictment is returned against an accused person, the court, through a judicial officer, will if appropriate or necessary issue a warrant for the arrest of the accused. Because there already was an arrest warrant for Jones based upon the charges in the Criminal Complaint against him, the Honorable Patty Shwartz, a United States Magistrate Judge for the United States District Court for the District of New Jersey, issued a second arrest warrant for Jones on April 28, 2011. The second arrest warrant is based upon the charges against Jones in the indictment. I have obtained from the Deputy Clerk of Court a certified true and accurate copy of the arrest warrant issued on April 28, 2011 and have attached it to this affidavit as **Exhibit B**. This arrest warrant remains valid and executable to apprehend Jones for the charges in the indictment.

D. Status of Co-defendants and their Alleged Roles in the Conspiracy

12. At this writing:

a. Defendant Karlis Karklins, a citizen of Latvia, is the subject of a request for provisional arrest to the Latvian government. I have executed an affidavit in support of an extradition request to the Republic of Latvia, which will be delivered to the Latvian government at the same time as the extradition request for Jones. The indictment alleges that defendant Karklins was involved in stealing personal information from victims and distributing that information to United States-based coconspirators who would assist in withdrawing money from compromised accounts.

b. Defendant Charles Chidi, believed to be a citizen of the United Kingdom, is at large and the subject of an arrest warrant in the United States. The indictment alleges that defendant Chidi was involved in stealing personal information from victims and distributing that information to United States-based coconspirators who would assist in withdrawing money from compromised accounts.

c. Defendant Waya Nwaki, a United States citizen, is at large and the subject of an arrest warrant in the United States. The indictment alleges that defendant Nwaki received stolen information from defendant Karklins and recruited others to withdraw money from compromised accounts.

d. Defendant Osarhieme Obaygbona, a United States citizen, is in custody in the District of New Jersey and is pending trial. The indictment alleges that defendant Obaygbona received stolen information from defendant Nwaki and recruited others to withdraw money from compromised accounts.

e. Defendant Alphonsus Osuala, a Nigerian citizen, is in custody in Atlanta, Georgia on unrelated charges. The Indictment alleges that defendant Osuala obtained and shared personal identifiers that were used together with stolen information to make withdrawals from compromised accounts.

f. Defendant Marvin Dion Hill, a United States citizen, was arrested in the United States on or about July 1, 2011 and is pending trial in the District of New Jersey. The Indictment alleges that defendant Hill obtained and shared personal identifiers that were used together with stolen information to make withdrawals from compromised accounts.

E. Overview of the Case

13. Between in or about August 2009 and in or about June 2010, Jones, his six co-defendants, Karlis Karklins, Charles Chidi, Waya Nwaki, Osarhieme Obaygbona, Marvin Dion Hill, and Alphonsus Osuala, and other coconspirators worked together across three continents as part of a conspiracy that attempted to steal approximately US\$3.2 million from payroll companies and banks. To do so, Karklins, Chidi, and other members of the conspiracy used Internet “phishing” attacks and bogus websites to trick unwitting consumers into giving up their online usernames and passwords.

14. After obtaining these credentials, Karklins, Chidi, and other members of the conspiracy added fake employees to the payroll accounts of victim companies at payroll processing companies. They used these victims’ online accounts to “pay” the fake employees through electronic transfers. Karklins, Chidi, Nwaki, Obaygbona, Osuala, Hill and Jones then divided up the proceeds by transferring them to accounts that they controlled and by wiring money overseas via bank wire, Western Union, and Moneygram.

15. The FBI’s investigation revealed that Jones had two specific roles in the conspiracy. First, he opened bank accounts in Nigeria into which the fraudulent proceeds of the scheme were wired. Second, using a fraud commonly known as a “romance scam,” Jones impersonated a young European woman online in order to trick men into believing that they were having an online romantic relationship with a “Brenda Stuart.” Jones used e-mail accounts in Brenda Stuart’s name to trick these “Money Mules” (as they are described in the Indictment) into sending overseas the proceeds of the fraud that his conspirators deposited into the Money Mules’ bank accounts.

F. The Phishing Fraud and Wire Transfers to John Massoni

16. In phishing attacks, on-line criminals create fraudulent websites and e-mails that mimic the legitimate websites and e-mails of e-Commerce providers (such as banks and payroll processors) in an attempt to trick unwitting computer users — who believe that they are dealing with legitimate websites — into divulging their confidential information (such as passwords, user names, and account numbers). The confidential information, once stolen, can be used in furtherance of computer crimes that involve unauthorized access to online accounts.

17. The FBI's investigation revealed that ADP and Intuit were American companies that offered corporate customers the ability to manage their payroll accounts over the Internet. ADP customers could, for example, upon providing the appropriate username and password, add employees to their payroll and direct that money (i.e., salary) be transferred to those employees.

18. In approximately January 2010, intruders gained unauthorized access to two computers in Florida and uploaded phishing webpages that purported to be on-line account access screens for ADP. The phishing webpages appeared legitimate and included ADP's trademarked logo, but they were in fact fraudulent. Legitimate ADP customers were tricked into visiting the fraudulent website, where they were prompted for user names and passwords as if they were accessing ADP's legitimate website.

19. According to a network administrator responsible for one of the Florida computers, once customers unwittingly entered their user names and passwords onto the fraudulent websites, those user names and passwords were forwarded automatically to an e-mail address using the Internet domain e-serveclub.com, among other e-mail addresses.

20. In March 2010, the FBI received additional reports from ADP of phishing-related activities targeting its customers. Specifically, an ADP account manager received an e-mail from the e-mail account SusanNeon@gmail.com ("the SusanNeon Gmail Account") asking why a particular ADP customer's payroll had been suspended. The account manager, who was generally familiar with phishing scams, suspected fraud because the customer referenced in the e-mail from the SusanNeon Gmail Account was not within that manager's region.

21. The FBI's investigation established links between the January 2010 phishing pages placed on the Florida computer servers and the March 2010 e-mail ADP. Specifically, a Latvian IP address was used to connect to the Florida computers and to log-in to the SusanNeon Gmail Account.

22. On approximately April 1, 2010, pursuant to a court order, the FBI obtained and searched the contents of the SusanNeon Gmail Account. At that time, the SusanNeon Gmail Account contained approximately 3,500 e-mails dating between approximately August 2009 and March 2010. The account contained, among other evidence:

- a. images of web pages used in furtherance of phishing attacks on ADP, Chase Bank, and other e-Commerce companies;
- b. instructions on how to access the computer located in Pennsylvania to which stolen account credentials had been e-mailed from the Florida computers involved in the January 2010 phishing attacks;
- c. e-mails describing the fraudulent addition of employees to ADP-run payroll accounts;

- d. e-mail "scripts" describing, in step-by-step detail, how to contact ADP by telephone and have payroll issued on behalf of non-existent employees;
- e. usernames and passwords for ADP customers; and
- f. account numbers and on-line credentials for customers of Intuit.

23. As described below, conspirators caused ADP (and other payroll processors) to issue payroll in the names of fictitious employees onto prepaid Ecount debit cards. (Ecount, a subsidiary of Citigroup, sells prepaid debit cards onto which employers, including customers of ADP and Intuit, can transfer payroll amounts instead of using traditional paychecks or directly depositing the funds into an employee's bank account.)

24. For example, on March 3, 2010, the SusanNeon Gmail Account was used to send the following e-mail, in substance and in part, to the e-mail address usaprince12k@gmail.com, which was controlled by defendant Waya Nwaki:¹

CALL TO (714) 690-7083

IF THEY ASK THEN YOUR NAME IS:

H***** M*****

YOU ARE THE CONTROLLER

UR PHONE IS 848-***-0**1

EMAIL IS H*M@****.COM (if they wanna mail ****, its okay. i can acess [sic] this email)

If they ask about the new payrolls, tell you have submited [sic] today 6 payrolls total

1) Three payrolls to M***** G*****, each 10k, if she ask why, tell her because Online payroll didnt [sic] allow to do more than 10k per one transfer

2) One payroll to E***** W***** - 9k with something

3) Three payrolls to J*****

¹This affidavit replaces portions of the confidential personal identifiers of victims with "*" symbols.

on T***** - each 10k, if she ask why - tell her because ONline payroll didnt allow to do more than 10k per one transfer

If they ask about:

M***** G*****

J**** TH****

E***** W*****

Tell them that these are new contractors that you added today and that it is very important that the payment will process today.

company details

Company name: **-* INTERNATIONAL LTD

Legal address: 1227 ***** STREET

City: *****

State: CALIFORNIA

Business Phone: 858-***-0**1

25. The FBI's investigation revealed that the telephone number listed at the top of the March 3 e-mail, (714) 690-7083, was an ADP client service manager's phone number. In addition, that same day, ADP officials reported having received instructions over the company's website regarding the payroll accounts that are described in the March 3 e-mail — those of "M.G.", "E.W.", and "J.T." ADP was also directed on that date to issue payroll in the exact amounts described in the March 3 email message (*i.e.*, "three payrolls to [J.T.] — each \$10k").

26. Records obtained from Ecount show that on approximately March 4, 2010, an account established in the name of "J.T." received three US\$10,000 deposits from the ADP customer, **-* INTERNATIONAL LTD, which is the California company named in the March 3 email message.

27. Ecount records further revealed that on approximately March 4, 2010, US\$30,000 was withdrawn from J.T.'s Ecount account, and wired to a Sovereign Bank account in the name of John Massoni ("Massoni"), a resident of New York City, with an account number ending in 7106.

28. Sovereign Bank records, obtained pursuant to a subpoena, revealed that on March 8, 2010, approximately US\$26,585 was wired from Massoni's account to Ecobank, a Nigerian bank, for the benefit of an account in the name of Olaniyi Victor Makinde, which is an alias Jones uses.

29. The FBI identified several other fraudulent transactions that originated with compromised ADP or Intuit user accounts, transferred money through Ecount to John Massoni's Sovereign Bank Account, and then concluded with Massoni wiring money to either Ecobank or Intercontinental Bank accounts that Jones controlled. These transfers are both among the objects of the wire fraud conspiracy described in Count 1 of the Indictment and the substantive wire fraud charges in Counts 2 through 5 of the Indictment.

30. These transfers included, among others:

a. A March 8, 2010 transfer of approximately US\$26,585 to Jones' Ecobank account that was funded by unauthorized payroll withdrawn from the ADP payroll account of a company identified in the Indictment as "Company A." This wire transfer in furtherance of the phishing scheme is charged as Count 2 of the Indictment.

b. A February 18, 2010 transfer of approximately US\$29,000 to Jones' Intercontinental Bank account that was funded by unauthorized payroll withdrawn from the ADP payroll account of a law firm identified in the Indictment as "Law Firm C".

This wire transfer in furtherance of the phishing scheme is charged as Count 3 of the Indictment.

c. A February 11, 2010 transfer of approximately US\$20,690 to Jones' Ecobank account that was funded by unauthorized payroll withdrawn from ADP payroll account of a victim identified in the Indictment as "Corporation D". This wire transfer in furtherance of the phishing scheme is charged as Count 4 of the Indictment.

d. An October 21, 2009 transfer of approximately US\$13,400 to Jones' Ecobank account that was funded by unauthorized payroll withdrawn from the Intuit payroll account of a victim. This wire transfer in furtherance of the phishing scheme is charged as Count 5 of the Indictment.

31. In total, Sovereign Bank records show that between in or about July 2009 and in or about April 2010, Massoni wired at least approximately US\$303,000 to Jones' accounts at Ecobank and Intercontinental Bank.

G. Jones and the Brenda Stuart Romance Scam

32. Pursuant to Court orders in furtherance of its investigation, the FBI obtained e-mails between Massoni and two e-mail accounts: BSBrendaStuartBS@gmail.com ("the BSBrenda Stuart Account") and BrendaStuart@rocketmail.com ("the Brenda Stuart Rocketmail Account") (collectively "the Brenda Stuart Accounts"). The FBI also obtained copies of e-mails sent from and to the Brenda Stuart Accounts.

33. Review of the Brenda Stuart Accounts shows that "Brenda Stuart" was an alias that Jones adopted to trick men like Massoni into wiring stolen money overseas. More specifically, these accounts show that Jones represented "Brenda Stuart" to be European woman seeking romantic ties. Money Mules, after communicating online with "Brenda Stuart" and

receiving provocative photographs of a white woman matching “Brenda Stuart’s” description, would frequently be asked to send money to Jones via Western Union, Moneygram, or wire transfer to Ecobank and Intercontinental Bank. In e-mails from the Brenda Stuart Account, Jones often characterized the payments as necessary to help an ailing family member or to assist Brenda Stuart in otherwise legitimate business activity.

34. In Massoni’s case, on or about January 19, 2009, Jones used the BSBrendaStuart Account to send the following e-mail to Massoni:

IM Brenda Stuart.. Im French...I have my mom here who stays with me.
She is 66 and Im her only daughter..so I make sure I take a very good care of her..
as she needs support My Dad is late... They are from Paris.. France and they took
me down to the US when I was 12 and since then ..I have been here.. I had my
university of California, Los angeles where I had my BEng in Architecture and
interior designs,... and I look forward to having my MBA.. etc.....
I have nothing or NO friends.. I do some travellings when I have to.. I have been
to a couple of countries in Europe.. !
I am into commercial and residential designs but much into commercial.. Im
independent contractor and I work with firms and private individuals at their
demand for my service..
I have knowledge of italian and german designs..... Oopps
What more

Jones also sent approximately 37 photos of white female in her mid-20s.²

35. The next day, January 20, 2009, Jones sent a second e-mail from the BSBrenda Stuart account under the header “My Private Pics...” This second e-mail contained approximately 18 pictures of the same woman, but this time the woman in the photographs was unclothed and in various provocative poses in a shower.

²Notably, review of the BSBrendaStuart Account shows that between approximately August 2008 and January 2009, Jones sent the same e-mail, in substance and in part, to hundreds of online accounts. Based on my review of many of these e-mails, it appears that Jones posted a Yahoo! Personals advertisement to which many of his victims responded via e-mail.

36. Review of the e-mails between the BSBrendaStuart Account and John Massoni show that an online relationship ensued. On January 22, 2009, for example, Massoni wrote to the BSBrenda Stuart Account that he thought he had found his "one true love." Jones responded that day that Brenda Stuart "love[d] you [Massoni] so much."

37. On or about January 22, 2009, Jones replied as Brenda Stuart, asking Massoni to send him money.

Thanks honey and I feel the same way about u
when are u getting me the 500\$ that I needed for my return?
You should borrow it from your landlord or get it from your son
Love you and You excite me so much as well and this is why I want to return
asap.. for us to meet in person rather than chatting online at all times..
Love you

Sincerely,
Brenda Stuart

38. The e-mails between Massoni and Jones continued through 2009, with "Brenda Stuart" repeatedly asking Massoni to send money abroad. In one instance, on or about February 6, 2009, Jones asks Massoni to send US\$250 via Western Union to an Andrea Bradley, 2 Dallimore Street, Ijapo Estate, Akure, Ondo State, Nigeria ("the Dallimore Street Address"). The Dallimore Street Address appears throughout the BS Brenda Stuart Account as a receiving address for Western Union and Moneygram wire transfers. (The FBI later learned that Andrea Bradley was an alias Jones stated he used, and that Jones had previously lived at the Dallimore Street Address.)

39. In a July 2009 e-mail requesting that Massoni send money via Moneygram, "Brenda Stuart" identified an "Olaniyi Jones" as her "roommate," and provided the Dallimore Street Address as the receiving address for a Moneygram overseas wire.

Communications Regarding Wire Transfers to Ecobank and Intercontinental Bank

40. On or about October 20, 2009, Jones used the BSBrenda Stuart Account to send the following e-mail to John Massoni:

Hi My Love.
I am Glad you finally got the poem that I resent back to you.
I had problems in searching for it and that was why it took a bit long. sorry about that.
I came online to look for u in the afternoon today but I didnt see you online.
IF and when you find a payment of 13700\$ in your acct tommorrow.. its mine honey.
I will talk to u later today.
IF you are not online.. I will send u an email

Love you,

Brenda

41. Sovereign Bank records reveal that the next day, October 21, 2010, Massoni sent a US\$13,400 payment to Jones' Ecobank account.

42. Similarly, on or about November 5, 2011, Jones used the BSBrenda Stuart Account to send the following e-mail to John Massoni:

Hi Honey,
IF you see some 10,000\$ in your acct.. its mine.. take \$150 from it and wire the rest to the SAME acct mi amor.. Thanks

Yours

Brenda

43. The same day, on or about November 5, 2011, Sovereign Bank records show that Massoni sent US\$9,750 to Jones Ecobank account.

H. Additional Connections Between the Phishing Fraud and Jones

44. The FBI's review of the contents of the SusanNeon Gmail Account used to further the phishing fraud against ADP showed additional connections between the "phishing fraud" and Jones' communications with Massoni.

45. First, a December 29, 2009 e-mail in the SusanNeon Gmail Account contained Massoni's name and New York address under the header "USA Item Drop." There is accordingly cause to believe that defendant Karklins, who coordinated the phishing attacks against ADP, Intuit, and others, was aware that Massoni was the intended recipient of items furthering the fraud.

46. Second, an October 23, 2009 e-mail to the SusanNeon Gmail Account from the e-mail address Lakes.Sider80@gmail.com contained a scanned copy of a wire transfer confirmation regarding a US\$13,400 wire transfer from John Massoni's Sovereign Bank account to an Ecobank account in the name of Olaniyi Victor Makinde. This e-mail appears to relate to the wire transfer from Massoni to Jones described in paragraphs 40 and 41 above. The FBI therefore believes that the owner of the SusanNeon Gmail Account — identified in the Indictment as Karlis Karklins, a Latvian citizen — was receiving notice of a successful transfer to Jones of money stolen in furtherance of the crimes charged in the Indictment.³

47. Third, at the time of his arrest in September 2010, described below, Jones' cell phone contained what appear to be bank account numbers for Guaranty Trust Bank attributed to "Lakes," the same nickname with whom defendant Karklins was communicating with regarding

³The BSBrendaStuart account regularly communicated with the e-mail address Lakes.Sider80@gmail.com, as well as other e-mail accounts beginning with "Lakes" and "lakes.sider," regarding Massoni and other money mules.

the phishing fraud. There is accordingly cause to believe that an unknown individual with the alias Lakes (or a variant of Lakes) acted as an intermediary between Jones and Karklins.

48. Fourth, according to information obtained from the Latvian government, on or about January 8, 2010, defendant Karklins received an approximately USD\$2,400 wire transfer from a Guaranty Trust Bank account in the name of Akinnola Gbenga Christopher. Two days earlier, on January 6, 2010, defendant Jones had received an approximately US\$15,000 wire transfer of fraudulent proceeds from Massoni. Similarly, on or about February 5, 2010, the same day that Jones received an approximately US\$20,000 wire transfer of fraudulent proceeds from Massoni, defendant Karklins' bank account received an approximately US\$750 (USD) wire transfer from a United Bank for Africa account in the name of Ismaila Raimi Olalekan. These transfers indicate some temporal and financial relationship between defendant Karklins and Nigeria as defendant Jones is receiving in Nigeria the proceeds of the fraud that defendant Karklins initiated.

49. Finally, a June 3, 2010 e-mail from the BSBrenda Stuart Account contains an Internet chat transcript between "Lakes Inc" and a "Victor Niyi Jones." In the chat, "Victor Niyi Jones" states:

Victor Niyi Jones: I was like make them go carry massoni

Victor Niyi Jones: but that FBI bros come ask hin brother

Victor Niyi Jones: say which work I dey do... say this is US and NOT Nigeria

Victor Niyi Jones: I come reason say

Victor Niyi Jones: if them carry massoni

Victor Niyi Jones: he fit start to dey confess

Victor Niyi Jones: and they will trace ALL Past TRANSACTIONS of his acct

Victor Niyi Jones: come my side

Victor Niyi Jones: come link my acct to my efcc and put my face for efcc net as
WANTED

(emphasis supplied). The FBI believes that this chat, based on the reference to “past transactions” of Massoni’s account coming to “my side,” was typed by the owner of the Ecobank and Intercontinental Bank accounts to which Massoni wired money. “Lakes” is again believed to be an intermediary between Jones and Karklins, who handled the Internet phishing attacks that enabled the scheme to wire money to Jones.

I. The Identification of Jones as the User of the Brenda Stuart Accounts

50. In or about June 2010, the FBI sent an information request to the Economic & Financial Crimes Commission regarding the accounts at Ecobank and Intercontinental Bank to which Massoni was wiring what appeared to be fraudulent proceeds.

51. In or about September 2010, the FBI learned that the EFCC had arrested Jones on local charges on September 6, 2010 after Jones appeared at Ecobank, one of the banks to which Massoni had been wiring fraudulent proceeds.

52. On approximately October 12, 2010, FBI agents traveled to Lagos, Nigeria in connection with their investigation of the offenses charged in the indictment. While in Lagos, the FBI agents interviewed Jones at the Economic and Financial Crime Commission, Lagos Office, 15A Awolowo Road, Ikoyi, Lagos, Nigeria.

53. The FBI agents, who were accompanied at the interview by representatives of the EFCC, interviewed Jones.

54. In substance and in part, Jones stated:

a. prior to his arrest, he resided at 19 Arisoyim Street, Akura; Jones used the e-mail address makindev@yahoo.co.uk;⁴

⁴Notably, an October 8, 2009 e-mail from the BSBrendaStuart Account contained wiring instructions for an Ecobank account in the name of OLANIYI VICTOR MAKINDE. That e-mail was carbon copied to, among other e-mail addresses, makindev@yahoo.co.uk, the e-mail account

b. In approximately February or March 2009, Jones obtained a Nigerian driver's license bearing his picture and the name Andrea Bradley. (As noted below, an e-mail account in the name of Andrea Bradley was supplied to Intercontinental Bank in opening one of the two accounts that received the proceeds of the phishing scheme).

c. Jones opened bank accounts at Ecobank Nigeria, PLC, Intercontinental Bank, Zenith Bank, and Oceanic Bank. (As noted above, the Ecobank Nigeria, PLC and Intercontinental Bank accounts that Jones opened received fraudulent proceeds from the phishing scheme).

d. Beginning in approximately September 2009, Jones received U.S. dollar wire transfers from a John Massoni, although he had never met Massoni. (As noted above, John Massoni was the Money Mule that "Brenda Stuart" persuaded to transfer stolen proceeds to Jones' accounts).

e. At the instruction of a third party, Jones deposited the money he received into accounts at Skye Bank, Guaranty Trust Bank, United Bank for Africa, of Bank PHB (Platinum Habib Bank).

f. Jones believed the money he received from Massoni to be the proceeds of fraud.

g. Jones received more than US\$200,000 (US) from Massoni but kept only approximately 20,000 Nigerian naira (approximately US\$130 at this writing).

h. On or about July 24, 2008, Jones opened an Intercontinental Bank account (account number 0028201000000140) in the name Olaniyi Jones, at address 2 Dallimore Street, Ijapo Estate, Akure, Ondo State, with contact e-mail address

that Jones stated he used.

Andrea Bradley ny@yahoo.com. Jones admitted to using the alias Olaniyi Jones and to providing the Andrea Bradley e-mail account to Intercontinental Bank;⁵

i. Jones used to live at 2 Dallimore Street, Ijapo Estate, Akure, Ondo State; and

j. he and his family members were the individuals pictured in approximately eight family photographs dated March 2009 that appeared in the brendastuart@rocketmail.com e-mail account and in approximately two pictures dated January 2010 that appeared in the bsbrendastuartbs@gmail.com email account (providing reason to believe that Jones controlled the brendastuart@rocketmail.com and bsbrendastuartbs@gmail.com e-mail accounts).

55. While in Nigeria, FBI agents obtained from the EFCC a forensic copy of Jones' cell phone seized at the time of his arrest. That phone contained text messages exchanged with individuals in the United States who believed that they communicating with Brenda Stuart, including communications from victims who communicated with Brenda Stuart via e-mail to the BSBrendaStuartBS@gmail.com and BrendaStuart@rocketmail.com accounts. Many of the American individuals' names and contact information matched information found in the BS Brenda Stuart Account and the Brenda Stuart Rocketmail Account. This causes the FBI to believe that Jones was impersonating Brenda Stuart and was using the Brenda Stuart Accounts. As noted above, the cell phone also contained apparent banking information for "Lakes," which is consistent with the use of Lakes.Sider80@gmail.com and other e-mail and Internet chat accounts beginning with "lakes" in furtherance of the crimes charged in the Indictment.

⁵The name Andrea Bradley and the address 2 Dallimore Street, Ijapo Estate, Akure, Ondo State appears dozens of times as the recipient name and address in connection with Western Union and Moneygram transactions that "Brenda Stuart" forwarded to Money Mules.

J. Applicable Statutes and Discussion of the Elements of the Crimes

56. The statutes cited in the indictment and those applicable to this case are Title 18, United States Code, Section 1343 (wire fraud); Title 18, United States Code, Section 1349 (conspiracy); and Title 18, United States Code, Section 1028 (identity theft). A violation of any of these statutes is a felony under United States law. In addition, the accused person may be held liable under Title 18, United States Code, Section 2 for aiding and abetting the commission of the substantive felonies. Each of these statutes was the duly enacted law of the United States at the time that the offenses were committed, at the time the indictment was filed, and are now in effect. Copies of these statutes are attached as **Exhibit C**.

Conspiracy to Commit Wire Fraud (Count 1)

57. Under United States law, a conspiracy is an agreement to commit one or more criminal offenses. The agreement on which the conspiracy is based need not be expressed in writing or in words, but may be simply a tacit understanding by two or more persons to do something illegal. Conspirators enter into a partnership for a criminal purpose in which each member or participant becomes a partner or agent of every other member. A person may become a member of a conspiracy without full knowledge of all of the details of the unlawful scheme or the identities of all the other members of the conspiracy. If a person has an understanding of the unlawful nature of a plan and knowingly and willfully agrees to it, joining in the plan, he is guilty of conspiracy even though he did not participate before and may play only a minor part. A conspirator can be held criminally responsible for all reasonably foreseeable actions undertaken by other conspirators in furtherance of the criminal partnership.

58. Moreover, because of this partnership, statements made by a conspirator in the course of and while he is a member of the criminal conspiracy are admissible in evidence not only against that conspirator, but also against all other members of the conspiracy. This is so because, as stated earlier, a conspirator acts as an agent or representative of the other conspirators when he is acting in furtherance of their illegal scheme. Therefore, statements of conspirators made in furtherance of the conspiracy may be deemed to be the statements of all conspirators.

59. The crime of conspiracy is an independent offense, separate and distinct from the commission of any specific "substantive crimes." Consequently, a conspirator can be found guilty of the crime of conspiracy to commit an offense even where the substantive crime that was the purpose of the conspiracy is not committed. The Congress of the United States has deemed it appropriate to make conspiracy, standing alone, a separate crime, even if the conspiracy is not successful, because collective criminal planning poses a greater threat to the public safety and welfare than individual conduct and increases the likelihood of success of a particular criminal venture.

60. To prove the conspiracy charge in Count 1 of the indictment, the United States must show that:

- a. an agreement to commit wire fraud was entered into by two or more people;
- b. Jones knew the purpose of this unlawful agreement; and
- c. Jones knowingly joined the conspiracy.

Wire Fraud (Counts 2 through 5)

61. Jones is alleged in Count 1 of the indictment to have conspired to commit wire fraud, in violation of Title 18, United States Code, Section 1349. Additionally, he is charged in Counts 2 through 5 of the indictment with the substantive crime of wire fraud, in violation of Title 18, United States Code, Section 1343. The elements of wire fraud are that:

- a. Jones knowingly devised a scheme to defraud or to obtain money or property by materially false or fraudulent pretenses, representations or promises;
- b. he acted with the intent to defraud; and
- c. in advancing, furthering, or carrying out the scheme, Jones transmitted any writing, signal, or sound by means of a wire, radio, or television communication in interstate or foreign commerce or caused the transmission of any writing, signal, or sound of some kind by means of a wire, radio, or television communication in interstate or foreign commerce.

62. A “scheme to defraud” includes any scheme to deprive another of money or property by means of false or fraudulent pretenses, representations, or promises. An “intent to defraud” means an intent to deceive or cheat someone. A representation is “false” if it is known to be untrue or is made with reckless indifference as to its truth or falsity. A false statement is “material” if it has a natural tendency to influence, or is capable of influencing, the decision of the person or entity to which it is addressed. It is not necessary that the government prove all of the details alleged in the indictment concerning the precise nature and purpose of the scheme, or that the mailed material was itself false or fraudulent, or that the alleged scheme actually

succeeded in defrauding anyone, or that the use of the mail was intended as the specific or exclusive means of accomplishing the alleged fraud.

63. To “cause” the use of a wire communication is to do an act with knowledge that the use of a wire communication will follow in the ordinary course of business or where such use can reasonably be foreseen even though the defendant did not intend or request the use of a wire communication. Each separate use of a wire communication in furtherance of a scheme to defraud constitutes a separate offense. “Interstate or foreign commerce” means commerce or travel between one state, territory or possession of the United States and another state, territory or possession of the United States, including the District of Columbia. “Commerce” includes travel, trade, transportation and communication. Foreign commerce means commerce or travel between any part of the United States, including its territorial waters, and any other country, including its territorial waters. Under U.S. law the affect on interstate or foreign commerce can be minimal to satisfy this element. This element is satisfied in this case because of the e-mails sent by Jones and the wire transfers of the funds he caused to be sent which were between locations in the United States and Nigeria.

Identity Theft Conspiracy (Count 10)

64. Jones is alleged in Count 10 of the indictment to have conspired to commit identity theft, in violation of Title 18, United States Code, Section 1028(b)(1).

65. The elements of identity theft conspiracy are that:

- a. that two or more persons knowingly agreed to transfer or use in interstate or foreign commerce means of identification of another person without lawful authority

with the intent to commit, or aid or abet, any federal crime (which in this case is the wire fraud conspiracy) or any felony under State or local law;

- b. Jones knew the purpose of this unlawful agreement;
- c. Jones knowingly joined the conspiracy.

66. Under Title 18, United States Code, Section 1028, the term “means of identification” includes any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual,” including any “unique electronic identification number, address, or routing code.” These means of identification include, names, dates of birth, Social Security numbers, account numbers, and user log-in names and passwords as defined by Title 18, United States Code, 1028(d)(7). In this case, the conspirators trafficked in this type of information that they had obtained through phishing attacks.

Aiding and abetting and the law of principals (Counts 2 through 5)

67. Title 18, United States Code, Section 2, is the provision under U.S. law stating that a person who aids or abets another in the commission of a felony is guilty of the felony itself. To establish that a person is liable as an aider and abettor, the government must prove that:

- a. Jones knew that the crime charged was to be committed or was being committed;
- b. he knowingly did some act for the purpose of aiding, commanding, or encouraging the commission of that crime; and
- c. he acted with the intention of causing the crime charged to be committed.

68. This means that the guilt of an accused person may also be proved even if he did not personally perform every act involved in the commission of the crime charged. The law

recognizes that, ordinarily, anything a person can do for himself may also be accomplished through direction of another person as an agent, or by acting together with, or under the direction of, another person or persons in a joint effort. So, if the acts or conduct of an agent, employee or other associate of the accused person were willfully directed or authorized by the accused person, or if the accused person aided and abetted another person by willfully joining together with that person in the commission of a crime, then the law holds the accused person responsible for the conduct of that other person just as though the accused person had engaged in such conduct himself.

The Statute of Limitations

69. The statute of limitations on prosecuting the charged offenses is set forth in Section 3282 of Title 18, United States Code, which states:

Except as otherwise expressly provided by law, no person shall be prosecuted, tried, or punished for any offense, not capital, unless the indictment is found or the information is instituted within five years next after such offense shall have been committed.

70. The statute of limitations merely requires that an accused person be formally charged within five years of the date that the offense or offenses were committed. Once an indictment has been filed in a federal district court, as with these charges against Jones, the statute of limitations is tolled and no longer runs. This prevents a criminal from escaping justice by simply hiding out and remaining a fugitive for an extended period of time. Moreover, under the laws of the United States, the statute of limitations for a continuing offense, such as conspiracy, begins to run upon the conclusion of the conspiracy, not upon the commencement of the conspiracy.

71. I have thoroughly reviewed the applicable statute of limitations, and the prosecution of the charges in this case is not barred by the statute of limitations. Since the applicable statute of limitations is five years, and the indictment, which charges criminal violations occurring from on or about August 2009 through in or about July 2010, was filed on April 28, 2011, the defendant was formally charged within the specified five-year time period. I have also included as part of **Exhibit C** the true and accurate text of Title 18, United States Code, Section 3282.

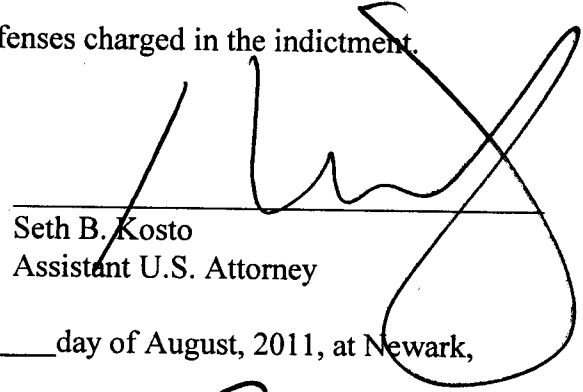
K. Identification

72. Jones is a citizen of Nigeria. He was born on February 15, 1982 in Nigeria. Jones is a black male who is approximately 167 centimeters tall, weighing approximately 68 kilograms, with black hair and brown eyes.

73. Jones has not been tried or convicted of the offenses charged in the indictment, nor has he been sentenced to serve any term of imprisonment in connection with this case. Photographs of Jones are attached as **Exhibits D** and **E**, respectively. The photographs of Jones in **Exhibit D**, in which Jones is the only subject wearing a bowtie, were obtained from Court-authorized searches of the Brenda Stuart Accounts used in furtherance of the offenses charged in the Indictment. The photograph of Jones in **Exhibit E** was taken by members of the EFCC prior to the FBI and EFCC's October 2010 interview of Jones in Lagos, Nigeria. FBI Special Agent R. Derek Rick, who participated in the October 2010 interview of Jones, advised me that the individual in a bowtie pictured in Exhibit D and the only individual pictured in Exhibit E was the Olaniyi Jones that FBI and EFCC agents interviewed in October 2010.


L. Conclusion

This affidavit was sworn to before a United States Magistrate Judge of the United States District Court for the District of New Jersey, who is legally authorized to administer an oath for this purpose. I have thoroughly reviewed this affidavit and the attachments to it, and attest that this evidence indicates that Jones is guilty of the offenses charged in the indictment.



Seth B. Kosto
Assistant U.S. Attorney

Signed and sworn to before me this 9 day of August, 2011, at Newark,
New Jersey in the District of New Jersey.



HONORABLE MARK FALK
United States Magistrate Judge

Exhibit List

Exhibit A	Certified Copy of Indictment
Exhibit B	Certified copy of arrest warrant
Exhibit C	Relevant Statutes
Exhibit D	Photograph of Jones obtained from e-mail account
Exhibit E	Photograph of Jones

EXHIBIT A

SBK/2009R00542

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEYUNITED STATES OF AMERICA
v.

KARLIS KARKLINS,
a/k/a "Susanne O'Neill,"
a/k/a "Kris,"
a/k/a "Steven Bing,"
CHARLES UMEH CHIDI,
a/k/a "Charlie,"
WAYA NWAKI,
a/k/a "Jonh Done,"
a/k/a "Prince Abuja,"
a/k/a "Shawn Conley,"
a/k/a "USAPrince12k,"
OSARHIEME UYI OBAYGBONA,
a/k/a "Uyi Obaygbona,"
a/k/a "bside bside,"
MARVIN DION HILL,
a/k/a "Da Boss,"
a/k/a "Nyhiar Da Boss,"
a/k/a "Nihiar Springs,"
ALPHONSUS OSUALA,
a/k/a "Andrew Johnson,"
a/k/a "jamal j," and
OLANIYI JONES,
a/k/a "Brenda Stuart,"
a/k/a "Olaniyi Victor Makinde,"
a/k/a "Makinde Olaniyi Victor"

Hon. *(WJM)*
Criminal No. 11-299
18 U.S.C. § 1343
18 U.S.C. § 1349
18 U.S.C. § 1028(f)
18 U.S.C. § 1028A(a)(1)
18 U.S.C. § 1030(a)(4)
18 U.S.C. § 1030(b)
18 U.S.C. § 2

I HEREBY CERTIFY that the above and
foregoing is a true and correct copy of
the original on file in my office.

ATTEST
WILLIAM T. WALSH, Clerk
United States District Court
District of New Jersey

By: *Marion Dwyer* 7/28/11
Deputy Clerk

INDICTMENT

The Grand Jury in and for the District of New Jersey,
sitting at Newark, charges:

I HEREBY CERTIFY that the above and
foregoing is a true and correct copy of
the original on file in my office.

ATTEST
WILLIAM T. WALSH, Clerk
United States District Court
District of New Jersey

COUNT 1
18 U.S.C. § 1349
(Conspiracy to Commit Wire Fraud)
(All Defendants) 8/9/11

By: *Lorraine McPerry*
Deputy Clerk

BACKGROUND

1. Between in or about August 2009 and in or about June

2010, the seven defendants named in this Indictment worked together across three continents in an effort to steal millions of dollars. To do so, the defendants used Internet "phishing" attacks and bogus websites to trick unwitting consumers into giving up their online usernames and passwords.

2. Armed with these credentials, defendants added fake employees to the payroll accounts of victim companies at payroll processing companies. They used these victims' online accounts to "pay" the fake employees through electronic transfers. Defendants then divided up the proceeds by transferring them to accounts that they controlled and by wiring money overseas via bank wire, Western Union, and Moneygram.

3. Defendants also used the stolen credentials to access customers' online bank accounts, to gather personal information about their victims, and to make fraudulent withdrawals from the victims' bank accounts. Defendants again divided the proceeds and wired funds overseas.

4. At various times relevant to this Indictment:

Defendants

a. Defendant KARLIS KARKLINS, a/k/a "Susanne O'Neill," a/k/a "Kris," a/k/a "Steven Bing," resided in or near Riga, Latvia. Defendant KARKLINS used the e-mail account susanneon@[Provider 1].com ("the Susan Neon Account"), among other e-mail accounts.

b. Defendant CHARLES UMEH CHIDI, a/k/a "Charlie," resided in the United Kingdom. Defendant CHIDI used the e-mail account Carl_Jay@[Provider 3].co.uk.

c. Defendant WAYA NWAKI, a/k/a "Jonh Done," a/k/a "Prince Abuja," a/k/a "Shawn Conley," a/k/a "USAPrince12k," resided in or near Atlanta, Georgia. Defendant NWAKI used the e-mail accounts usaprincl2k@[Provider 1].com and usaprincl2k@[Provider 2].com, among other e-mail accounts.

d. Defendant OSARHIEME UYI OBAYGBONA, a/k/a "Uyi Obaygbona," a/k/a "bside bside," resided in or near Atlanta, Georgia. Defendant OBAYGBONA used the e-mail account htownniggas@[Provider 2].com.

e. Defendant MARVIN DION HILL, a/k/a "Da Boss," a/k/a "Nihiar Springs," a/k/a "Nyhiar Da Boss," resided in or near College Park, Georgia. Defendant HILL used the e-mail accounts nahnahgetmoney@[Provider1].com and nyhiar@[Provider1].com.

f. Defendant ALPHONSUS OSUALA, a/k/a "Andrew Johnson," a/k/a "jamal j," resided in or near Atlanta, Georgia. Defendant OSUALA used the e-mail account aldandy_22@[Provider2].com.

g. Defendant OLANIYI JONES, a/k/a "Brenda Stuart," a/k/a "Olaniyi Victor Makinde," a/k/a "Makinde Olaniyi Victor," resided in Nigeria. Defendant JONES used the e-mail accounts bsbrendastuartbs@[Provider 1].com and brendastuart@[Provider

31.com, among other e-mail accounts.

Other Individuals

h. J.M., who is not charged as a defendant in this Indictment, resided in New York City. Defendant JONES, posing as "Brenda Stuart," e-mailed J.M. in order to deceive him into believing that "Brenda Stuart" was an American woman who was romantically interested in J.M. After receiving provocative and intimate e-mails and photographs from "Brenda Stuart," J.M. received and wired proceeds of the fraud to overseas bank accounts that defendant JONES controlled.

Corporations

i. Automated Data Processing, Inc., headquartered in Essex County, New Jersey ("ADP"); Intuit, Inc., headquartered in California ("Intuit"); and other payroll processing companies (collectively, "the Payroll Processors") provided outsourcing of human resources, payroll, tax and benefits administration services. The Payroll Processors offered customers the ability to manage their payroll accounts over the Internet. Upon providing the appropriate username and password (hereinafter, "Log-In Credentials") at the Payroll Processors' public-facing websites, customers could add employees to their payroll and pay those employees.

j. Ecount, a subsidiary of Citigroup, sold prepaid debit cards onto which employers, including customers of the

Payroll Processors, could transfer payroll amounts instead of using traditional paychecks or direct deposit ("Payroll Debit Cards").

k. Bank of America and JPMorgan Chase Bank ("Chase Bank") were financial institutions within the meaning of Title 18, United States Code, Section 20. Bank of America and Chase Bank were among the country's largest retail financial institutions and offered extensive consumer credit, checking, and savings products that provided customers online access to their accounts.

Definitions

1. In "phishing" attacks, online criminals create fraudulent websites and e-mails that mimic the legitimate websites and e-mails of e-Commerce providers (such as banks, payroll processors, and utilities) in an attempt to trick unwitting computer users - who believe that they are dealing with legitimate websites - into divulging their Log-In Credentials and other personally identifying information, such as dates of birth, Social Security Numbers, addresses, telephone numbers, mother's maiden names, and responses to online security questions ("Personal Identifiers"). The Log-In Credentials and Personal Identifiers, once stolen, can be used in furtherance of computer crimes that involve unauthorized access to online accounts.

m. "Spear phishing" attacks are phishing attacks

where online criminals select their victims using knowledge of the victims' existing account relationships. The attack depends upon the premise that impersonating communications from ADP, for example, is a far more effective tactic when communications are sent to ADP customers (a spear phishing attack) than if they are sent indiscriminately to employers nationwide (a phishing attack).

THE CONSPIRACY

5. Between in or about August 2009 and in or about June 2010, in the District of New Jersey and elsewhere, defendants

KARLIS KARKLINS,
a/k/a "Susanne O'Neill,"
a/k/a "Kris,"
a/k/a "Steven Bing,"
CHARLES UMEH CHIDI,
a/k/a "Charlie,"
WAYA NWAKI,
a/k/a "Jonh Done,"
a/k/a "Prince Abuja,"
a/k/a "Shawn Conley,"
a/k/a "USAPrince12k,"
OSARHIEME UYI OBAYGBONA,
a/k/a "Uyi Obaygbona,"
a/k/a "bside bside,"
MARVIN DION HILL,
a/k/a "Da Boss,"
a/k/a "Nyhiar Da Boss,"
a/k/a "Nihiar Springs,"
ALPHONSUS OSUALA,
a/k/a "Andrew Johnson,"
a/k/a "jamal j," and
OLANIYI JONES,
a/k/a "Brenda Stuart,"
a/k/a "Olaniyi Victor Makinde,"
a/k/a "Makinde Olaniyi Victor"

did knowingly and intentionally conspire with each other and

others to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, and sounds, contrary to Title 18, United States Code, Section 1343.

OBJECT OF THE CONSPIRACY

6. It was the object of the conspiracy for defendants KARKLINS, CHIDI, NWAKI, OBAYGBONA, HILL, OSUALA, and JONES and others to steal money from payroll processors and banks by using phishing and spear phishing attacks to obtain Log-In Credentials and Personal Identifiers that were used to make unauthorized withdrawals from customers' online accounts.

MANNER AND MEANS OF THE CONSPIRACY

The Phishing Attacks

7. It was part of the conspiracy that defendants KARKLINS and CHIDI and others designed and deployed on the Internet fraudulent web pages ("Phishing Pages") that resembled the public-facing websites of payroll processing companies and banks ("the E-Commerce Companies").

8. It was further part of the conspiracy that defendants

KARKLINS and CHIDI and others caused phishing and spear phishing e-mails to be sent to the E-Commerce Companies' customers ("the Customers") in an attempt to trick the Customers into visiting the Phishing Pages. These e-mails appeared to be legitimate but were actually fraudulent e-mails that contained electronic links to the Phishing Pages. Those Customers who clicked on the electronic links were directed automatically to the Phishing Pages, where they saw what appeared to be the trademarked logos of the E-Commerce Companies and were prompted for and entered their Log-In Credentials and Personal Identifiers.

9. It was further part of the conspiracy that defendants KARKLINS and CHIDI and others caused any Log-In Credentials and Personal Identifiers that Customers typed into Phishing Pages to be intercepted and transmitted, not to the E-Commerce Companies, but to computers and e-mail accounts that defendants KARKLINS and CHIDI and others controlled.

Using the Stolen Log-In Credentials and Personal Identifiers

10. It was further part of the conspiracy that defendants KARKLINS, CHIDI, NWAKI, OBAYGBONA, HILL, and OSUALA and others emailed Log-In Credentials and Personal Identifiers that they had obtained to each other and others in exchange for payment or the promise of payment.

11. It was further part of the conspiracy that defendants KARKLINS, NWAKI, HILL, and others contacted the E-Commerce

Companies by telephone and over the Internet and used stolen Log-In Credentials and Personal Identifiers to impersonate the Customers and to obtain additional Personal Identifiers.

12. It was further part of the conspiracy that defendants KARKLINS and NWAKI and others used stolen Log-In Credentials and Personal Identifiers to cause fraudulent withdrawals to be made from the Customers' accounts at the E-Commerce Companies ("the Fraudulent Withdrawals").

Distributing the Proceeds of the Scheme

13. It was further part of the conspiracy that defendant KARKLINS and others caused some of the Fraudulent Withdrawals to be deposited onto Ecount Payroll Debit Cards and into other bank accounts that they controlled.

14. It was further part of the conspiracy that defendants KARKLINS and JONES and others caused the proceeds of some of the Fraudulent Withdrawals to be transferred to bank accounts belonging to individuals they employed ("Money Mules").

15. It was further part of the conspiracy that defendants KARKLINS and JONES caused the Money Mules to transfer funds out of the United States, sometimes by persuading the Money Mules that they were wiring money in furtherance of romantic relationships or professional opportunities.

16. It was further part of the conspiracy that defendants KARKLINS, CHIDI, NWAKI, HILL, JONES and others shared the

proceeds of the Fraudulent Withdrawals through wire transfers to individuals and bank accounts that they controlled in the United States, Mexico, the United Kingdom, Latvia, France, Bulgaria, Russia, and Nigeria, among other countries.

17. In this fashion, defendant KARKLINS, CHIDI, NWAKI, OBAYGBONA, HILL, OSUALA, and JONES and others attempted to obtain at least approximately \$3.5 million in Fraudulent Withdrawals, and did make at least approximately \$1.3 million in Fraudulent Withdrawals.

FRAUDULENT ACTIVITY

18. In order to further the object of the conspiracy, defendants KARKLINS, CHIDI, NWAKI, HILL, OBAYGBONA, OSUALA, and JONES and others conducted the following fraudulent activity in the District of New Jersey and elsewhere:

Phishing and Spear Phishing

a. On or about November 11, 2009, defendant KARKLINS e-mailed defendant CHIDI under the subject header "HOST INFO" ("the November 11 E-Mail"). The November 11 E-Mail contained Internet Protocol addresses, a user name, and a password that together provided administrative access (i.e., the ability to upload or download files over the Internet) to a computer located in Scranton, Pennsylvania that was used to store Phishing Pages and stolen Log-In Credentials and Personal Identifiers.

b. On or about November 12, 2009, defendant KARKLINS sent

an e-mail under the header "Chase Scam" ("the Chase Scam E-Mail") to the e-mail address lakes.sider80@[Provider1].com ("the Lakes Sider 80 Account"). The Chase Scam E-Mail contained an image of a Phishing Page resembling a public facing website of Chase Bank.

c. On or about November 12, 2009, defendant KARKLINS e-mailed the Lakes Sider 80 Account under the subject header "msg" ("the Msg E-Mail"). The Msg E-Mail attached a phishing e-mail that purported to come from Chase Bank requesting that customers "upgrade" their accounts "for security reasons" by clicking on an electronic link.

d. On or about December 9, 2009, defendant KARKLINS created an e-mail attaching the Chase Scam E-Mail and a Phishing Page that impersonated a public-facing website of Chase Bank.

e. On or about January 12, 2010, defendant KARKLINS created an e-mail containing a Phishing Page that impersonated a public-facing website of ADP.

f. On or about January 12, 2010, defendant KARKLINS created and sent three e-mails containing approximately 27 sets of ADP and e-mail Log-In Credentials under the subject header "ADPs from SPAM" and "ADP."

Attacks Targeting Payroll Processors and their Customers

The H.M. Transaction

g. On or about March 4, 2010, at approximately 12:09 a.m. (GMT), defendant KARKLINS e-mailed defendant NWAKI and instructed

him to telephone ADP and to impersonate "H.M.," the controller of ADP customer "Company A," and to request that ADP issue approximately \$69,000 in payroll checks to three purported Company A.O. employees: "M.G.," "E.W.," and "J.T."

h. Approximately 30 minutes later, defendant NWAKI e-mailed defendant HILL and instructed defendant HILL to telephone ADP, to impersonate H.M., and to cause ADP to issue approximately \$69,000 in payroll checks to M.G., E.W., and J.T. Defendant NWAKI instructed defendant HILL, in part:

Why u must call is that u must make her process the payroll for march 4. That's what u start the conversation wit..that u want to what to do to process the march 4 payrolls.

i. On or about March 4, 2010, defendants KARKLINS, NWAKI, and HILL and others accessed ADP's public-facing website and caused ADP to issue approximately \$60,000 in payroll on behalf of Company A.O. to M.G., E.W. and J.T., including by transferring approximately \$30,000 to an Ecount Payroll Debit Card in the name of J.T. ("the J.T. Ecount Card").

j. On or about March 4, 2010, defendants KARKLINS, NWAKI and HILL and others caused approximately \$30,000 to be wired from the J.T. Ecount Card to a Sovereign Bank account in the name of J.M. ("the J.M. Sovereign Account").

k. On or about March 8, 2010, defendant JONES caused J.M. to wire approximately \$26,500 from the J.M. Sovereign Account to an account at Ecobank, a Nigerian bank, that defendant JONES

controlled ("the Ecobank Account").

The D.C. Transaction

l. On or about February 16, 2010, defendant KARKLINS e-mailed Log-In Credentials associated with the payroll account of "Law Firm C," an ADP customer, to lakes.sider70@[Provider 1].com ("the Lakes Sider 70 Account").

m. On or about February 16, 2010, defendant KARKLINS and others caused ADP to initiate four fraudulent payroll transfers of approximately \$10,000, each on behalf of Law Firm C, to an Ecount Payroll Debit Card in the name of D.C., a purported employee who had been added to Law Firm C's payroll account at ADP ("the D.C. Ecount Card").

n. On or about February 17, 2010, defendant KARKLINS and others caused Ecount to transfer approximately \$40,000 from the D.C. Ecount Card to the J.M. Sovereign Account.

o. On or about February 18, 2010, the day after the funds arrived in the J.M. Sovereign Account, defendant JONES caused J.M. to wire approximately \$29,000 from the J.M. Sovereign Account to an account at Intercontinental Bank, a Nigerian bank, that defendant JONES controlled ("the Intercontinental Account").

p. On or about February 18, 2010, defendant KARKLINS exchanged e-mails with an attorney at Law Firm C in which defendant KARKLINS purported to seek legal advice regarding a pending criminal charge.

q. On or about February 21, 2010, defendant JONES forwarded to the Lakes Sider 70 Account an e-mail from J.M. reporting that J.M. had forwarded approximately \$29,000 to the Intercontinental Account.

The B.B. Transaction

r. On or about January 26, 2010, a coconspirator used the Lakes Sider 80 Account to create an e-mail containing the Log-In Credentials of an ADP customer, "Corporation D."

s. On or about January 28, 2010, a coconspirator used the Lakes Sider 80 Account to create an e-mail containing the Log-In Credentials and Personal Identifiers of an individual identified herein as "B.B."

t. On or about February 5, 2010, a coconspirator fraudulently caused ADP to wire, on behalf of its customer, Corporation D, approximately \$21,000 to an Ecount Payroll Debit Card in the name of B.B., a purported employee who had been added to Corporation D's payroll account at ADP ("the B.B. Ecount Card").

u. On or about February 8, 2010, a coconspirator transferred approximately \$21,700 to the J.M. Sovereign Account.

v. On or about February 11, 2010, defendant JONES caused J.M. to transfer approximately \$20,700 to the Ecobank Account.

w. On or about February 11, 2010, defendant JONES e-mailed to the Lakes Sider 80 Account confirmation of an approximately

\$20,700 wire transfer from the J.M. Sovereign Account.

Impersonating a Company F Representative

x. On or about March 11, 2010, defendant KARKLINS e-mailed an ADP client service manager. KARKLINS represented himself to be a representative of Company F, an ADP customer, inquiring why payroll had been suspended on Company F's account.

y. On or about March 11, 2010, a coconspirator fraudulently caused ADP to wire, on behalf of its customer Company F, approximately \$40,000 to an Ecount Payroll Debit Card in the name of J.H., a purported employee who had been added to Corporation F's payroll account at ADP.

The J.M. Sovereign Account Wire Confirmation

z. On or about October 21, 2009, defendant JONES caused J.M. to wire approximately \$13,400 obtained from Intuit from the J.M. Sovereign Account to the Ecobank Account ("the October 21 Wire").

aa. On or about October 23, 2009, an unknown coconspirator used the Lakes Sider 80 Account to e-mail defendant KARKLINS a scanned copy of a Sovereign Bank wire transfer confirming the October 21 Wire.

bb. Between in or about July 2009 and in or about April 2010, defendant JONES caused J.M. to send at least approximately

\$300,000 from the J.M. Sovereign Account to defendant JONES in Nigeria.

Attacks Targeting Banks

K.J.W.

cc. On or about September 17, 2009, defendant KARKLINS e-mailed defendant CHIDI the Log-In Credentials and Personal Identifiers of the Chase Bank customer "K.J.W." under the subject header "The Login!!! 30k lets make a lot \$\$\$\$."

dd. On or about September 21, 2009, defendants KARKLINS and CHIDI caused a Fraudulent Withdrawal of approximately \$13,000 from K.J.W.'s Chase Bank account.

ee. On or about November 18, 2009, defendant NWAKI e-mailed K.J.W.'s Log-In Credentials and Personal Identifiers to defendant OBAYGBONA under the subject header "Chase."

ff. On or about November 21, 2009, defendant KARKLINS e-mailed defendant NWAKI K.J.W.'s Log-In Credentials and Personal Identifiers under the subject header "28k chase, male, login yourself for check copy."

L.D.

gg. On or about October 21, 2009, defendant KARKLINS e-mailed defendant NWAKI under the subject header "Chase 23K Female with Check copy attached" ("the October 5 E-Mail"). The October 5 E-Mail contained Log-In Credentials, the Personal Identifiers,

and the bank account balance of "L.D." The October 5 E-Mail also attached an image of a check drawn on L.D.'s Chase Bank account.

hh. On or about October 21, 2009, defendant NWAKI e-mailed defendant HILL an image of the same check drawn on L.D.'s Chase Bank, L.D.'s Personal Identifiers and L.D.'s bank account balance.

ii. On or about October 22, 2009, defendants KARKLINS, NWAKI and HILL caused a Fraudulent Withdrawal of approximately \$5,000 from L.D.'s Chase Bank account.

R.R.

jj. On or about October 29, 2009, defendant KARKLINS e-mailed defendant NWAKI the Log-In Credentials and Personal Identifiers for the Chase Bank customer "R.R." and an image of a check drawn on R.R.'s Chase Bank account.

kk. On or about October 30, 2010, defendant KARKLINS and NWAKI caused a Fraudulent Withdrawal of approximately \$5,000 from R.R.'s Chase Bank checking account.

ll. On or about November 12, 2009, defendant NWAKI e-mailed R.R.'s Log-In Credentials, Personal Identifiers and an image of a check drawn on R.R.'s account to defendant OBAYGBONA.

K.M.

mm. On or about November 4, 2009, defendant KARKLINS e-mailed defendant NWAKI the Log-In Credentials and Personal Identifiers for the Chase Bank customer "K.M."

nn. On or about November 11, 2009, defendant NWAKI e-mailed K.M.'s Log-In Credentials and Personal Identifiers to defendant OBAYGBONA.

oo. On or about November 17, 2009, defendants KARKLINS, NWAKI, and OBAYGBONA caused a Fraudulent Withdrawal of approximately \$12,200 from K.M.'s Chase Bank account through purchases made at Atlanta-area retail stores.

S.M.

pp. On or about January 19, 2010, at approximately 8:00 p.m. (UTC), defendant NWAKI e-mailed defendant KARKLINS under the subject header "re: = CHASE 13.8k = male, age 32, check copy attached" the Log-In Credentials and Personal Identifiers of a Chase Bank customer named "S.M."

qq. On or about January 19, 2010, at approximately 11:30 p.m. (UTC), defendant KARKLINS created an e-mail under the subject header "2k Regions did to Wachovia [S.]" containing S.M.'s name and computer code evidencing unauthorized access to S.M.'s Chase Bank online account.

Gaining Unauthorized Access to Customers' Online Accounts

B.R.

rr. On or about November 15, 2009, defendant KARKLINS accessed an online Bank of America account belonging to "B.R.,"

and accessed screens related to "Safepass," an online security feature offered by Bank of America.

ss. That day, defendant KARKLINS sent an e-mail with the subject header "boa 26k + safepass added with the number u gave + mail access" to the Lakes Sider 80 Account that included Log-In Credentials and Personal Identifiers for "B.R.," including responses to the questions "What is your maternal grandmother's first name?" and "What is your mother's middle name?"

S.H.

tt. On or about December 30, 2009, defendant KARKLINS sent an e-mail under the header "boa business 25k + mail access" to AO7million@Provider11.com containing the Log-In Credentials and Personal Identifiers of a Bank of America customer, "S.H.", including account balances and responses to Bank of America security questions.

uu. On or about December 31, 2009, defendant KARKLINS gained unauthorized access to S.H.'s online Bank of America account and attempted to send approximately \$4,500 by wire to a bank account in Mexico.

R.J.K.

vv. On or about January 20, 2010, defendant KARKLINS e-mailed defendant NWAKI under the subject header "@Chase@Male, 22k, age 54, check copy attached - find dob urself" ("the January

20 E-Mail"). The January 20 E-Mail contained the Log-In Credentials and bank balance of a Chase Bank customer, "R.J.K." Defendant KARKLINS also attached an image of a check drawn on R.J.K.'s Chase account to the January 20 E-Mail.

ww. In a reply to the January 20 E-Mail on or about January 21, 2010, defendant NWAKI stated, in substance and in part, "on this one you f*ck up again. i can login into the account cuz u give me the wrong email address" Defendant KARKLINS replied, in substance and in part, "You have lame hands. IT WORKS BITCH".

J.K.

xx. On or about March 18, 2010, defendant OSUALA sent an e-mail to defendant NWAKI that contained the Log-In Credentials and Personal Identifiers of a Chase Bank customer, "J.K."

yy. On or about April 7, 2010, at approximately 6:06 p.m., defendant NWAKI sent an e-mail under the header "New chase ass" to defendant KARKLINS that contained J.K.'s Log-In Credentials and Personal Identifiers.

zz. On or about April 7, 2010, at approximately 6:20 p.m., defendant KARKLINS accessed J.K.'s Chase Bank online account without authorization.

aaa. On or about May 25, 2010, J.K.'s Chase Bank account received a fraudulent \$24,000 ACH deposit from Citibank. That day and the next day, more than \$24,000 was withdrawn from J.K.'s

account by a coconspirator.

M.H.

bbb. On or about April 5, 2010, defendant NWAKI sent an e-mail to defendant KARKLINS under the header "he changed the usid use this account" that contained the Log-In Credentials of a Chase Bank customer, "M.H.," to defendant KARKLINS.

ccc. On or about April 6, 2010, defendant KARKLINS accessed M.H.'s Chase Bank online account without authorization.

C.M.

ddd. On or about March 12, 2010, defendant NWAKI created an e-mail under the subject header "[C.M.]" that contained the Log-In Credentials and Personal Identifiers of a Chase Bank customer, "C.M."

eee. On or about April 5, 2010, defendant KARKLINS accessed C.M.'s Chase Bank online account without authorization.

fff. On or about April 21, 2010, defendant KARKLINS created an e-mail under the header "Chase Drops" containing C.M.'s Log-In Credentials and Personal Identifiers.

ggg. On or about June 30, 2010, defendant KARKLINS created an e-mail under the header "Chase Drops" containing C.M.'s Log-In Credentials and Personal Identifiers.

Trafficking in the Log-In Credentials and Personal Identifiers of New Jersey Residents

hhh. On or about November 21, 2009, defendant KARKLINS e-mailed defendant NWAKI the Log-In Credentials and Personal Identifiers of "B.S.," a Chase Bank customer who resided in New Jersey.

iii. On or about December 7, 2009, defendant KARKLINS e-mailed defendant NWAKI the Log-In Credentials and Personal Identifiers of "A.O.," a Chase Bank customer who resided in New Jersey.

Harvesting Personal Identifiers

jjj. On or about April 8, 2010 at 1:33 (GMT), defendant HILL e-mailed five names and addresses of individuals residing in Alpharetta or Cumming, Georgia to defendant NWAKI.

kkk. Approximately four hours later, at 6:08 (GMT), defendant NWAKI e-mailed the same five names and addresses to defendant KARKLINS under the subject "Pls get the ssn# n dob."

Sharing the Proceeds of the Conspiracy

lll. On or about February 19, 2010, defendant HILL opened a bank account at Regions Bank ("the Hill Regions Account").

mmm. On or about March 30, 2010, defendant KARKLINS e-mailed defendant NWAKI instructions to wire approximately \$2,700 to Bulgaria and approximately \$925 to Latvia.

nnn. On or about March 30, 2010, defendant HILL wired approximately \$2,600 via Western Union to Bulgaria to a recipient named "D.N.R."

ooo. On or about March 30, 2010, defendant NWAKI e-mailed defendant KARKLINS that defendant HILL had wired approximately \$2,600 to D.N.R. in Bulgaria. Defendant NWAKI further advised that approximately \$830 in additional funds had been sent to "G.G.," a recipient in Latvia.

ppp. On or about March 31, 2010, defendant NWAKI e-mailed defendant KARKLINS under the subject header "50k drop" with the Log-In Credentials for the Hill Regions Account.

qqq. On or about May 14, 2010, under the subject header "WU info's," defendant KARKLINS sent the following e-mail to defendant NWAKI:

Send 4170 USD (deduct fee's from his share) to:
First name: [V.]
Last name: [V.]
City: Sofia
Country: Bulgaria

DON'T USE PRINCE ABUJA NAME FOR THIS !!! -> Send 1390
USD (deduct fees from his share) to:
First name: [E.]
Last name: [G.]
City: Riga
Country: Latvia

rrr. Between in or about September 2009 and in or about December 2010, defendant KARKLINS and others in Latvia (whose names defendant KARKLINS e-mailed to defendant NWAKI) received approximately \$98,000 via Western Union.

sss. Between in or about July 2009 and in or about April 2010, defendant JONES caused J.M. to send at least approximately \$300,000 from the J.M. Sovereign Account to defendant JONES in Nigeria.

In violation of Title 18, United States Code, Section 1349.

COUNTS 2 THROUGH 5

18 U.S.C. § 1343

18 U.S.C. § 2

(Wire Fraud)

(Defendants KARKLINS, NWAKI, HILL and JONES)

1. Paragraphs 1 through 4 and 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. On or about the dates set forth below, in Essex County, in the District of New Jersey, and elsewhere, the defendants identified below and others did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud and to obtain money and property from the Payment Processors by means of materially false and fraudulent pretenses, representations, and promises, namely, through the manner and means described in paragraphs 7 through 17 of Count 1 of the Indictment, and for the purpose of executing such scheme or artifice, did knowingly transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, namely wire transfers from Sovereign Bank in the United States to various bank accounts in Nigeria in the approximate amounts described below.

COUNT	DEFENDANTS	DATE	AMOUNT	WIRE DESTINATION
2	KARKLINS NWAKI HILL JONES	03/08/2010	\$26,585	Ecobank
3	KARKLINS JONES	02/19/2010	\$28,334	Intercontinental

COUNT	DEFENDANTS	DATE	AMOUNT	WIRE DESTINATION
4	JONES	02/11/2010	\$20,692	Ecobank
5	KARKLINS JONES	10/21/2009	\$13,400	Ecobank

In violation of Title 18, United States Code, Section 1343
and Section 2.

COUNTS 6 THROUGH 9

18 U.S.C. § 1343

18 U.S.C. § 2

(Wire Fraud)

(Defendants KARKLINS, CHIDI, NWAKI, OBAYGBONA, and HILL)

1. Paragraphs 1 and 4 through 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. On or about the dates set forth below, in Essex County, in the District of New Jersey, and elsewhere, the defendants identified below and others did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud and to obtain money and property from JPMorgan Chase Bank by means of materially false and fraudulent pretenses, representations, and promises, namely, through the manner and means described in paragraphs 7 through 17 of Count 1 of the Indictment, and for the purpose of executing such scheme or artifice, did knowingly transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, namely, interstate and international emails containing Log-In Credentials and Personal Identifiers of the bank customers identified below sent in furtherance of Fraudulent Withdrawals in the approximate amounts identified below:

Count	Defendants	Date	Accountholder	Fraudulent Withdrawal
6	KARKLINS CHIDI	09/17/2009	"K.J.W."	\$13,000

Count	Defendants	Date	Accountholder	Fraudulent Withdrawal
7	KARKLINS NWAKI HILL	10/21/2009	"L.D."	\$5,000
8	KARKLINS NWAKI	10/29/2009	"R.R."	\$5,000
9	OBAYGBONA KARKLINS NWAKI	11/17/2009	"K.M."	\$12,203.56

In violation of Title 18, United States Code, Section 1343
and Section 2.

COUNT 10

18 U.S.C. § 1028(f)
(Conspiracy to Commit Identity Theft)
(All Defendants)

1. Paragraphs 1 through 4 and 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. Between at least as early as in or about August 2009 and in or about June 2010, in the District of New Jersey and elsewhere, defendants

KARLIS KARKLINS,
a/k/a "Susanne O'Neill,"
a/k/a "Kris,"
a/k/a "Steven Bing,"
CHARLES UMEH CHIDI,
a/k/a "Charlie,"
WAYA NWAKI,
a/k/a "Jonh Done,"
a/k/a "Prince Abuja,"
a/k/a "Shawn Conley,"
a/k/a "USAPrince12k,"
OSARHIEME UYI OBAYGBONA,
a/k/a "Uyi Obaygbona,"
a/k/a "bside bside,"
MARVIN DION HILL,
a/k/a "Da Boss,"
a/k/a "Nyhiar Da Boss,"
a/k/a "Nihiar Springs,"
ALPHONSUS OSUALA,
a/k/a "Andrew Johnson,"
a/k/a "jamal j," and
OLANIYI JONES,
a/k/a "Brenda Stuart,"
a/k/a "Olaniyi Victor Makinde,"
a/k/a "Makinde Olaniyi Victor"

did knowingly and intentionally conspire with each other and others to transfer, possess and use means of identification of other persons without lawful authority, in a manner affecting interstate and foreign commerce, with the intent to commit, and

in connection with, unlawful activity constituting a violation of federal law, namely, Title 18, United States Code, Section 1343, contrary to Title 18, United States Code, Sections 1028(a)(7).

In violation of Title 18, United States Code, Section 1028(b)(1).

COUNTS 11 THROUGH 19

18 U.S.C. § 1028A(a)(1)

18 U.S.C. § 2

(Aggravated Identity Theft)

(Defendants KARKLINS, CHIDI, NWAKI, HILL, OBAYGBONA, and OSUALA)

1. Paragraphs 1 through 4 and 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. On or about the dates set forth below, in the District of New Jersey and elsewhere, the defendants identified below did knowingly and intentionally transfer, possess, and use, without lawful authority, means of identification of other persons, namely, the Log-In Credentials and Personal Identifiers of the individuals identified below, during and in relation to the felony violation of Title 18, United States Code, Section 1349, that is charged in Count 1 of this Indictment.

Count	Defendants	Date	Person
11	KARKLINS NWAKI HILL	03/04/2010	"H.M."
12	KARKLINS	02/16/2010	"Law Firm C"
13	KARKLINS CHIDI OBAYGBONA	09/17/2009 to 11/21/2009	"K.J.W."
14	KARKLINS NWAKI HILL	10/5/2009 to 10/21/2009	"L.D."
15	KARKLINS NWAKI OBAYGBONA	10/29/2009 to 11/12/2009	"R.R."

32

Count	Defendants	Date	Person
16	OBAYGBONA KARKLINS NWAKI	11/04/2009 to 11/11/2009	"K.M."
17	KARKLINS NWAKI	11/21/2009	"B.S."
18	KARKLINS NWAKI	12/07/2009	"A.O."
19	OSUALA NWAKI	03/18/2010	"J.K."

COUNT 20

18 U.S.C. § 1030(b)
(Conspiracy to Gain Unauthorized Access to Computers)
(Defendants KARKLINS, CHIDI, NWAKI,
OBAYGBONA, HILL, and OSUALA)

1. Paragraphs 1 through 4 and 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. Between at least as early as August 2009 and in or about June 2010, in the District of New Jersey, and elsewhere, defendants

KARLIS KARKLINS,
a/k/a "Susanne O'Neill,"
a/k/a "Kris,"
a/k/a "Steven Bing,"
CHARLES UMEH CHIDI,
a/k/a "Charlie,"
WAYA NWAKI,
a/k/a "Jonh Done,"
a/k/a "Prince Abuja,"
a/k/a "Shawn Conley,"
a/k/a "USAPrince12k,"
OSARHIEME UYI OBAYGBONA,
a/k/a "Uyi Obaygbona,"
a/k/a "bside bside,"
MARVIN DION HILL,
a/k/a "Da Boss,"
a/k/a "Nyhiar Da Boss,"
a/k/a "Nihiar Springs," and
ALPHONSUS OSUALA,
a/k/a "Andrew Johnson,"
a/k/a "jamal j"

did knowingly and with intent to defraud conspire and agree with each other and others to access protected computers without authorization, namely the computer networks used in and affecting interstate and foreign commerce and communication owned by Bank of America and JPMorgan Chase Bank, and exceed authorized access,

and by means of such conduct to obtain information for purposes of private financial gain and to further the intended fraud and obtain things of value, contrary to Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), and(a)(4).

In violation of Title 18, United States Code, Section 1030(b).

COUNTS 21 THROUGH 27
 18 U.S.C. § 1030(a)(4)
 18 U.S.C. § 2
 (Unauthorized Access to Computers to Commit Fraud)
 (Defendants KARKLINS and NWAKI)

1. Paragraphs 1 through 4 and 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. On or about the dates set forth below, in Essex County, in the District of New Jersey, and elsewhere, defendants

KARLIS KARKLINS,
 a/k/a "Susanne O'Neill,"
 a/k/a "Kris,"
 a/k/a "Steven Bing," and
 WAYA NWAKI,
 a/k/a "Jonh Done,"
 a/k/a "Prince Abuja,"
 a/k/a "Shawn Conley,"
 a/k/a "USAPrince12k"

did knowingly and with intent to defraud access protected computers, namely the computer networks used in and affecting interstate and foreign commerce and communication owned by the banks identified below, without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained things of value, namely Fraudulent Withdrawals from customers' accounts:


Count	Defendant	Victim Accountholder	Victim Bank	Date
21	KARKLINS	"B.R."	Bank of America	11/15/09
22	KARKLINS	"S.H."	Bank of America	12/30/09

23	KARKLINS NWAKI	"S.M."	Chase Bank	01/19/10
24	KARKLINS NWAKI	"R.J.K."	Chase Bank	01/20/10
25	KARKLINS	"C.M."	Chase Bank	04/05/10
26	KARKLINS NWAKI	"M.H."	Chase Bank	04/06/10
27	KARKLINS NWAKI	"J.K."	Chase Bank	04/07/10

In violation of Title 18, United States Code, Sections
1030(a)(4) and 1030(c)(3)(A) and Section 2.

A TRUE BILL

FOREPERSON



PAUL J. FISHMAN
United States Attorney

CASE NUMBER: 11-CR-299(WJM)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA

v.

KARLIS KARKLINS,
a/k/a "Susanne O'Neill,"
a/k/a "Kris,"
a/k/a "Steven Bing,"
CHARLES UMEH CHIDI,
a/k/a "Charlie,"
WAYA NWAKI,
a/k/a "Jonh Done,"
a/k/a "Prince Abuja,"

a/k/a "Shawn Conley,"
a/k/a "USAPrincel2k,"
OSARHIEME UYI OBAYGBONA,
a/k/a "Uyi Obaygbona,"
a/k/a "bside bside,"
MARVIN DION HILL,
a/k/a "Da Boss,"
a/k/a "Nyhlar Da Boss,"
a/k/a "Nihlar Springs,"

ALPHONSUS OSUALA,
a/k/a "Andrew Johnson,"
a/k/a "jamal j," and
OLANIYI JONES,
a/k/a "Brenda Stuart,"
a/k/a "Olaniyi Victor
Makinde,"
a/k/a "Makinde Olaniyi
Victor"

INDICTMENT FOR VIOLATIONS OF

18 U.S.C. §§ 1343, 1349, 1028(f), 1028A(a)(1), 1030(a)(4), 1030(b) and 2

A True Bill,

Foreperson

PAUL J. FISHMAN

UNITED STATES ATTORNEY, NEWARK, NEW JERSEY

SETH B. KOSTO
ASSISTANT U.S. ATTORNEY
NEWARK, NEW JERSEY
(973) 645-2737

EXHIBIT B

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

WARRANT FOR ARREST

v.

Case Number: 11-299 (WJM)

KARLIS KARKLINS et al.

To: The United States Marshal
and any Authorized United States Officer

YOU ARE HEREBY COMMANDED to arrest OLANIYI JONES

and bring him or her forthwith to the nearest magistrate to answer a(n)

X Indictment Information Complaint Order of Court Violation Notice Probation Violation Petition

charging him or her with (brief description of offense)

wire fraud, conspiracy to commit identity theft, and conspiracy to commit wire fraud

in violation of Title 18, United States Code, Section(s) 1343, 1349, 1028(f), and
Section 2

Patty Shantz
Hon. Claire C. Geechi
Name of Issuing Officer

United States Magistrate Judge
Title of Issuing Officer

Patty Shantz
Signature of Issuing Officer

April 28, 2011 at Newark, New Jersey
Date and Location

Bail fixed at \$ _____ by _____

I HEREBY CERTIFY that the above and foregoing is a true and correct copy of the original on file in my office.

RETURN

ATTEST
WILLIAM T. WALSH, Clerk
United States District Court
District of New Jersey

This warrant was received and executed with the arrest of the above-named defendant at _____

8/14 By: [Signature]
Deputy Clerk

Date Received	Name and Title of Arresting Officer	Signature of Arresting Officer
Date of Arrest		

EXHIBIT C

EXHIBIT C

Exhibit C contains the applicable portions of statutes describing the offenses with which the defendant is charged, the statute of limitations, and the penalties the defendant faces if convicted. Ellipses and asterisks are used to indicate portions of the statutes which are omitted because these portions do not apply to the case against the defendant.

Title 18, United States Code, Section 1343. Fraud by wire, radio, or television

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

* * *

Title 18, United States Code, Section 1349. Attempt and conspiracy

Any person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

Title 18, United States Code, Section 1028. Fraud and related activity in connection with identification documents, authentication features, and information

(a) Whoever, in a circumstance described in subsection (c) of this section--

(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; . . .

shall be punished as provided in subsection (b) of this section.

(b) The punishment for an offense under subsection (a) of this section is--

(D) an offense under paragraph (7) of such subsection that involves the transfer, possession, or use of 1 or more means of identification if, as a result of the offense, any individual committing the offense obtains anything of value aggregating \$1,000 or more during any 1-year period;

(2) a fine under this title or imprisonment for not more than 5 years, or both, if the offense is--

(c) The circumstance referred to in subsection (a) of this section is that--

(3) either--

(A) the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means; . . .

(d) In this section and section 1028A--

(7) the term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any--

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device ;

(f) Attempt and conspiracy.--Any person who attempts or conspires to commit any offense under this section shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

Title 18, United States Code, Section 2. Principals

(a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.

(b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.

Title 18, United States Code, Section 3282. Offenses not capital

(a) **In general.** — Except as otherwise expressly provided by law, no person shall be prosecuted, tried, or punished for any offense, not capital, unless the indictment is found or the information is instituted within five years next after such offense shall have been committed.

* * *

EXHIBIT D

Subject: wedding

From: Brenda Stuart <brendastuart@rocketmail.com>

Date: Tue, 17 Mar 2009 15:04:36 -0700 (PDT)

To: stevenbulls@yahoo.com

there u go..

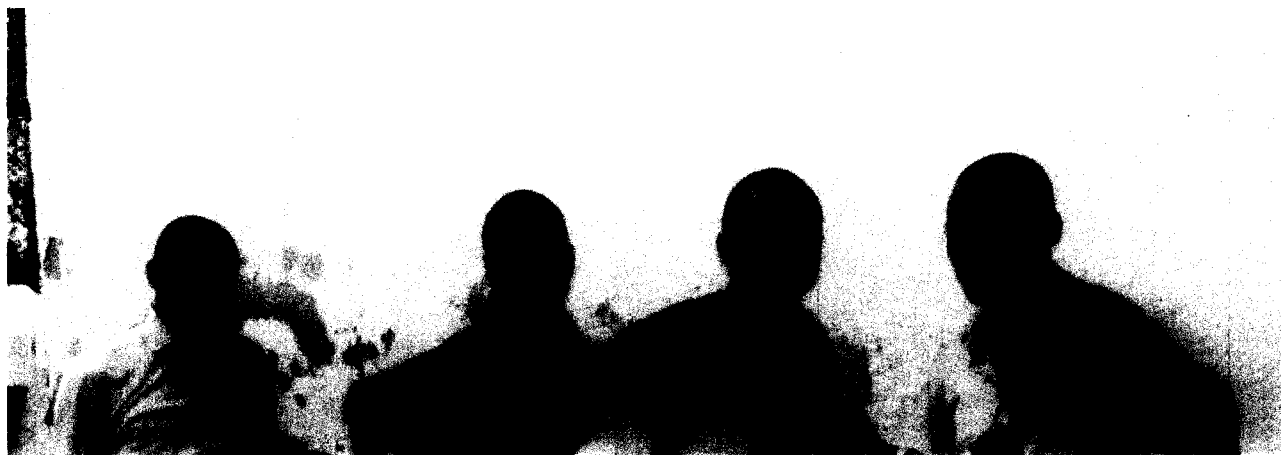
Sincerely,



Brenda Stuart



~~—Wedding 2..JPG—~~



~~—Wedding 3..JPG—~~



—Wedding 5..JPG—



—Wedding..JPG—



—Wedding..JPG—



Wedding 2..JPG	Content-Type: image/pjpeg Content-Encoding: base64
-----------------------	---

— Wedding 3..JPG —

Wedding 3..JPG	Content-Type: image/pjpeg Content-Encoding: base64
-----------------------	---

— Wedding 5..JPG —

Wedding 5..JPG	Content-Type: image/pjpeg Content-Encoding: base64
-----------------------	---

—Wedding..JPG—

Wedding..JPG	Content-Type: image/pjpeg Content-Encoding: base64
---------------------	---

—Wedding..JPG—

Wedding..JPG	Content-Type: image/pjpeg Content-Encoding: base64
---------------------	---

EXHIBIT E

